FORTINET
High Performance Network Security

FortiWLC

Release 8.3.3

Fortinet Wireless LAN Virtual Controllers

With this release of FortiWLC-SD, the FWC-VM Series Virtual Controllers - **FWC-VM-50, FWC-VM-200, FWC-VM-500, FWC-VM-1000**, and **FWC-VM-3000** are introduced.
For more information on deploying the Virtual controllers, see the *Virtual Controller Deployment Guide*.

Supported Hardware Configuration

The following table displays the minimum supported configuration for each of the virtual controller models.

Virtual Controller Model	Number of CPUs	RAM (GB)	vNIC
FWC-VM-50	4	4	1-4
FWC-VM-200	4	8	1-4
FWC-VM-500	8	16	1-4
FWC-VM-1000	24	32	1-4
FWC-VM-3000	48	64	1-8

Supported Virtual Platforms

With this release of FortiWLC-SD, the supported virtual platforms are VMware, Linux KVM, and Windows Hyper-V.

Note:

FWC-VM-1000 and FWC-VM-3000 Virtual Controllers **are not supported** on the Windows Hyper-V platform.

Fortinet Universal Access Points

This release of FortiWLC-SD introduces two new 802.11ac Wave2 access points, the FAP-U321EV and FAP-U323EV. The new Wave2 access points are dual radio, dual band 3x3 three stream 802.11ac Wave 2 access points designed to provide superior experience in data, voice, and video applications in enterprise class deployments.

FAP U321EV

FAP U323EV

FAP U323EV and FAP U321EV can be connected to 802.3at/802.3af PoE source.

FortiWLC 8.3.3 Upgrade/Install Files

The FortiWLC installation and upgrade files are available in a single directory in the release package.

These are the files for installing and upgrading the 64-bit virtual and hardware controllers.

Files	Description
forti-8.3-3GAbuild-0-x86_64-rpm.tar	Upgrades the 64-bit hardware controllers (FortiWLC-1000D and FortiWLC-3000D).
forti-8.3-3GAbuild-0-x86_64-vm-rpm.tar	Upgrades the 64-bit virtual controllers.
forti-8.3-3GAbuild-0-x86_64.img.KVM.zip	Installs 64-bit virtual controllers on the Linux KVM platform.
forti-8.3-3GAbuild-0-x86_64.ova	Installs 64-bit virtual controllers on the VMware platform.
forti-8.3-3GAbuild-0-x86_64.vhd.HV.zip	Installs 64-bit virtual controllers on the Windows Hyper-V platform.

Getting Started with Upgrade

The following table describes the approved upgrade path applicable for all controllers except the new virtual controllers. See the Installing 8.3.2 on Virtual Controllers section for specific instructions.

Note: FortiWLC-1000D and FortiWLC-3000D controllers can be upgraded only from 8.3 releases.

Supported Upgrade Releases

From FortiWLC release…	To FortiWLC Release…
7.0	7.0-10-0
8.0	8.0-5-0, 8.0-6-0
8.1	8.1-3-2
8.2	8.2.4
8.2.4/8.3	8.3.1
7.0.11, 8.2.7, 8.3.0, 8.3.1, and 8.3.2	8.3.3

Controller upgrade performed via CLI interface will require a serial or SSH2 connection to connect to the controller and use its CLI.

Check Available Free Space

Total free space required is the size of the image + 50MB (approximately 230 MB). You can use the **show file systems** command to verify the current disk usage.

```
controller# show file systems
Filesystem     1K-blocks   Used        Available   Use%   Mounted on
/dev/hdc2      428972      227844   178242      57%      /
none               4880          56            4824          2%       /dev/shm
```

The first partition in the above example, /hdc2, although the actual name will vary depending on the version of FortiWLC-SD installed on the controller is the one that must have ample free space.

In the example above, the partition shows 178242KB of free space (shown bolded above), which translates to approximately 178MB. If your system does not have at least 230MB (230000KB) free, use the **delete flash:<flash>** command to free up space by deleting older flash files until there is enough space to perform the upgrade (on some controllers, this may require deleting the flash file for the current running version).

Set up Serial Connection

Set the serial connection for the following options:

Only one terminal session is supported at a time. Making multiple serial connections causes signalling conflicts, resulting in damage or loss of data.

- Baud--115200
- Data--8 bits

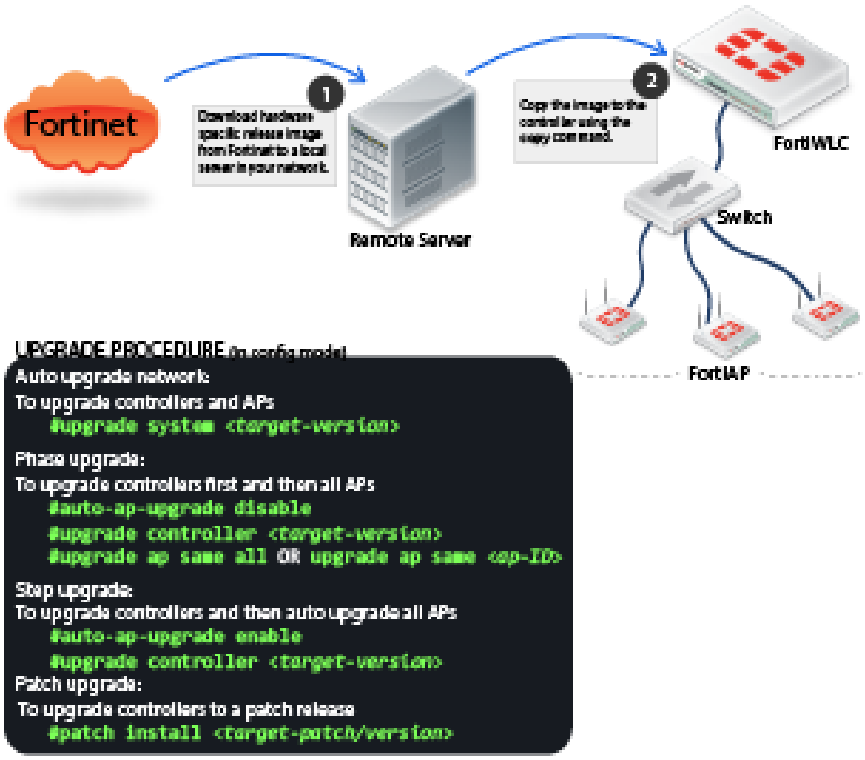
- Parity--None
- Stop Bit—1
- Flow Control—None

Supported Hardware and Software

Hardware and Software	Supported		Unsupported
Access Points	AP122 AP822e, AP822i (v1 & v2) AP832e, AP832i, OAP832e AP332e, AP332i* AP433e, AP433i, OAP433e* FAP U421EV FAP U423EV	FAP U321EV FAP U323EV AP1010e, AP1010i* AP1020e, AP1020i* AP1014i* AP110	AP201 AP208 AP150 AP300, AP301, AP302, AP302i, AP301i AP310, AP311, AP320, AP310i, AP320i OAP180 OAP380
*Cannot be configured as a relay AP			
Controllers	FortiWLC-50D FortiWLC -200D FortiWLC -500D FortiWLC- 1000D# FortiWLC -3000D# FWC- VM-50# FWC –VM-200# FWC –VM-500# FWC –VM-1000# FWC-VM-3000#	MC3200, MC3200-VE MC1550, MC1550-VE MC6000 MC4200 (with or without 10G Module) MC4200-VE	MC 5000 MC 4100 MC 1500 MC 1500-VE #Spectrum Manager NOT supported in these controller models
FortiWLM	8.3.3		
FortiConnect	16.8.2		
Browsers			
FortiWLC (SD) WebUI	Internet Explorer 9,10 Mozilla Firefox 25+ Google Chrome 31+		
A limitation of Firefox 3.0 and 3.5+ prevents the display of the X-axis legend of dashboard graphs.			
Captive Portal	Internet Explorer 6, 7, 8, 9, 10, IE11 and Edge. Apple Safari Google Chrome Mozilla Firefox 4.x and earlier Mobile devices (such as Apple iPhone and BlackBerry)		

Installing and Upgrading

The following instructions apply to FortiWLC-50D, FortiWLC-200D, FortiWLC-500D, MC1550, MC1550-VE, MC3200, MC3200-VE, MC4200, MC4200-VE and MC6000 controllers. See the Upgrading FortiWLC-1000D and FortiWLC-3000D and Installing 8.3.2 on new Virtual Controllers section for specific instructions. For upgrading the virtual controllers, see the *FortiWLC Virtual Controller Deployment Guide*.



1. Download image files from the remote server to the controller using one of the following commands:

```
# copy ftp://ftpuser:<password@ext-ip-addr>/<image-name-rpm.tar><space>.

[OR] # copy tftp://<ext-ip-addr>/<image-name-rpm.tar><space>.
```

   - **image-name** for legacy controllers: meru-{***release-version***}-{***hardware-model***}-rpm.tar. Eg, meru-***8.3-3-MC4200***-rpm.tar
   - **image-name** for FortiWLC: forti-{***release-version***}-{***hardware-model***}-rpm.tar. Eg, forti-***8.3-3-FWC2HD***-rpm.tar

2. Disable AP auto upgrade and then upgrade the controller (in config mode)

```
# auto-ap-upgrade disable

# copy running-config startup-config

# upgrade controller <target version> (Example, upgrade controller 8.3)
```

   The **show flash** command displays the version details.

3. Upgrade the APs

```
# upgrade ap same all
```

After the APs are up, use the **`show controller`** and **`show ap`** command to ensure that the controller and APs are upgraded to the latest (upgraded) version. Ensure that the system configuration is available in the controller using the **`show running-config`** command (if not, recover from the remote location). See the Backup Running Configuration step.

Upgrading FortiWLC-1000D and FortiWLC-3000D

To upgrade to 8.3.3 on FortiWLC-1000D and FortiWLC-3000D, use the following instructions:

Upgrading via CLI

1. Use the **show images**command to view the available images in the controller. By default, a new controller will boot from the primary partition which contains the running image.

```
default(15)# show images
Running image: Primary   <---- Denotes Primary Partition
--------------------------------------------------------------------------------
Running image details.
         System version: 0.3.2
         System hash: 11af7a3f3a700d3c8335dc254165282a91bd021b
         System branch: master
         System built: 20170323191620
         System memory: 721M/1006M
         Apps version: 8.3-1build-15
         Apps size: 1204M/1822M
--------------------------------------------------------------------------------
Other image details.
         System version: 0.3.3
         System hash: 4699cb9f517c4a2abbbce458f689bf3558b5d65e
         System branch: master
         System built: 20170511180827
         System memory: 729M/1015M
         Apps version: 8.3-1build-21
         Apps size: 1119M/1821M
```

2. To install the latest release, download the release image using the ***upgrade-image*** command:

```
upgrade-image scp://<username>@<remote-server-ip>:<path-to-image>/<image-name>-rpm.tar both reboot
```

The above command will upgrade the secondary partition and the controller will reboot to secondary partition.

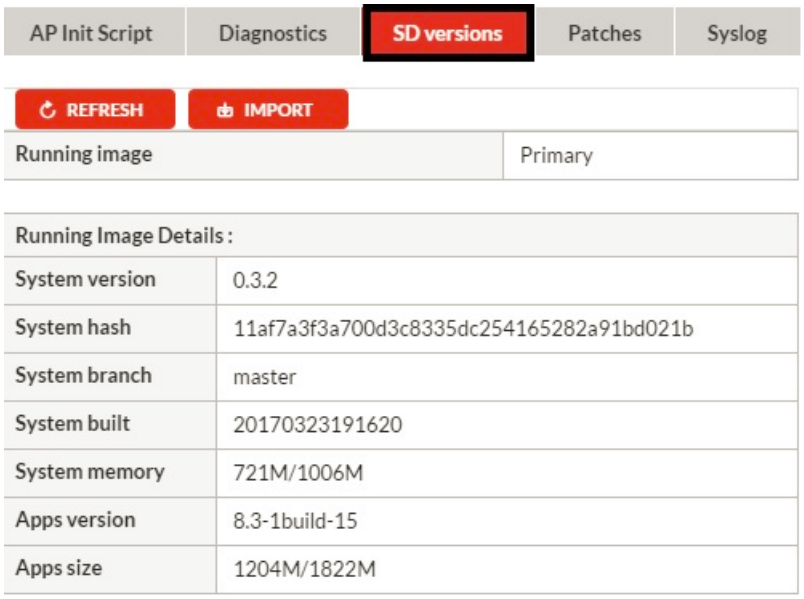
After an upgrade the current partition will shift to the second partition. For example, if you started upgrade in primary partition, post upgrade the default partition becomes secondary partition and vice- versa.

```
default(15)# show images
    Running image: Secondary  <-- Current partition after upgrade
    --------------------------------------------------------------------------------
    Running image details.
             System version: 0.3.2
             System hash: 11af7a3f3a700d3c8335dc254165282a91bd021b
             System branch: master
             System built: 20170323191620
             System memory: 729M/1015M
             Apps version: 8.3-1build-20
             Apps size: 1116M/1821M
```

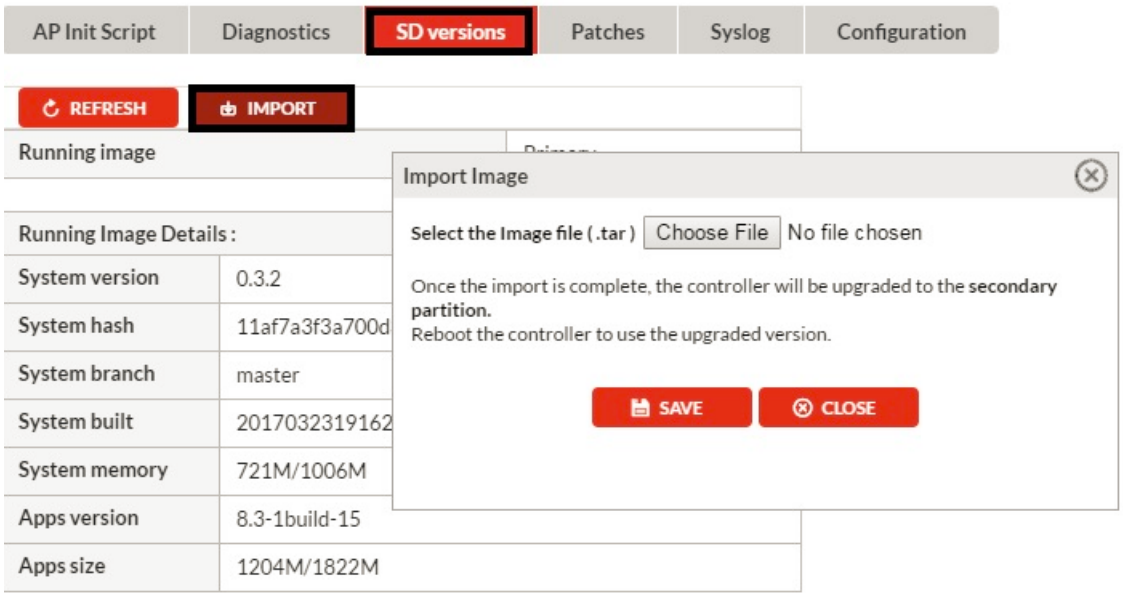
```
--------------------------------------------------------------------------------
Other image details.
         System version: 0.3.2
         System hash: 11af7a3f3a700d3c8335dc254165282a91bd021b
         System branch: master
         System built: 20170323191620
         System memory: 721M/1006M
         Apps version: 8.3-1build-15
        Apps size: 1204M/1822M
```

Upgrading via WebUI

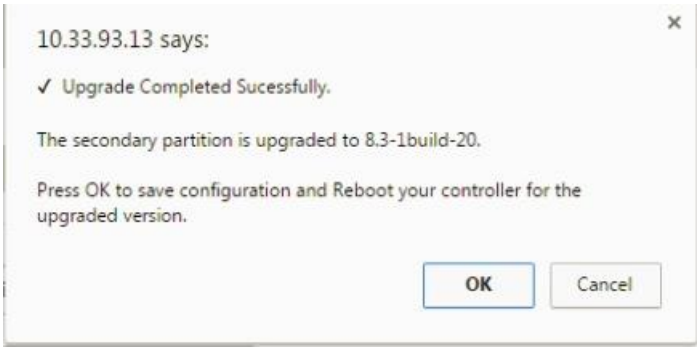
1. To upgrade controllers using WebUI, navigate to **Maintenance** > **File Management** > **SD Version**.



2. Click **Import** button to choose the image file.



3. After the import is complete, the following message is displayed



Switching Partitions

To switch partitions in FortiWLC-1000D, FortiWLC-3000D and the new virtual controllers, select the partition during the bootup process.

Upgrading a N+1 Site

To upgrade a site running N+1, all controllers must be on the same FortiWLC-SD version and the backup controller must be in the same subnet as the primary controllers. You can choose any of the following options to upgrade

- **Option 1** - Just like you would upgrade any controller, you can upgrade a N+1 controller.
  1. Upgrade master and then upgrade slave.
  2. After the upgrade, enable master on slave using the **`nplus1 enable`** command.
- **Option 2** - Upgrade slave and then upgrade master.
  After the upgrade, enable master service on slave using the **`nplus1 enable`** command
- **Option 3** - If there are multiple master controllers
  1. Upgrade all master controllers followed by slave controllers. After the upgrade, enable all master controllers on slave controllers using the **`nplus1 enable`** command.
  2. To enable master controller on slave controller, use the **`nplus1 enable`** command.
  3. Connect to all controllers using SSH or a serial cable.
  4. Use the **`show nplus1`** command to verify if the slave and master controllers are in the cluster.

The output should display the following information:

```
Admin:
Enable
Switch:
Yes
Reason:
-
SW Version: 8.3-1
```

5. If the configuration does not display the above settings, use the **nplus1 enable <master-controller-ip>** command to complete the configuration.
6. To add any missing master controller to the cluster, use the **nplus1 add master** command.

Restore Saved Configuration

1. Copy the backup configuration back to the controller:
   ```
   # copy ftp://<user>:<passswd>@<offbox-ip-address>/runningconfig.txt orig-config.txt
   ```
2. Copy the saved configuration file to the running configuration file:
   ```
   # copy orig-config.txt running-config
   ```
3. Save the running configuration to the start-up configuration:
   ```
   # copy running-config startup-config
   ```

Installing 8.3.3 on Virtual Controllers

Obtain a signed image file for the appropriate hypervisor module and install accordingly. A freshly installed system boots up as FWC-VM-50 with a default license valid for 30 days. After VM image installation, with all necessary resources allocated, VM is capable of emulating any virtual platform based on the product specific license.

No two Ethernet ports of virtual Controller should be connected to the same vSwitch since the port group in vSwitch is configured to be in promiscuous mode and hence both the ports will receive packets coming from all other ports in that vSwitch *including* the other port which is connected to the Controller.
For FWC-VM-3000, always connect all the ports to the VM switch. All the ports should be connected to different vSwitches whose uplinks should be connected to different ports on the external switch and all those ports should be link aggregated.

See License Management for Virtual Controllers section for importing licenses.

Upgrade Advisories

The following are upgrade advisories to consider before you begin upgrading your network.

Note:

Fortinet recommends upgrading a batch of maximum 100 APs.

Upgrading Virtual Controllers

In the Upgrade Command, select the options **Apps** or **Both** based on these requirements:

- Apps: This option will only upgrade the Fortinet binaries (rpm).
- Both: This option will upgrade Fortinet binaries as well as kernel (iso).

Mesh Deployments

When attempting to upgrade a mesh deployment, you must start upgrading the mesh APs individually, starting with the outermost APs and working inwards towards the gateway APs before upgrading the controller.

Feature Groups in Mesh profile

If APs that are part of a mesh profile are to be added to feature group, all APs of that mesh profile should be added to the same feature group. The Override Group Settings option in the ***Wireless Interface*** section in the Configuration > Wireless > Radio page must be enabled on the gateway AP.

Captive Portal and Fortinet Connect Deployment Recommendations

Since FortiWLC 8.3.3 fixes vulnerability issues, automatic configuration push from FortiConnect to FortiWLC does not work unless a patch is applied to FortiConnect 16.8. The patch is available at the Fortinet support site.

These are the deployment recommendations.

DNS Entry

It is mandatory to enter the DNS while creating internal DHCP profile.

External Portal IP Configuration

If a NAT device is located between the controller and the Fortinet Connect, the IP address with which Fortinet Connect sees the controller should be configured under Device > RADIUS Clients page in Fortinet Connect Admin portal (*http://<fortinetconnect-ip-address>/admin*) . Select the RADIUS client and enter the controller IP address in the Client tab. The Fortinet Connect Automatic Setup then configures the controller correctly and ensures that the correct controller IP address is configured on Fortinet Connect.

Remember Me settings

In the Portal Settings step of the Guest Portal configuration wizard, if you choose to enable Remember Credentials, then select "Initially attempt to use a cookie, if this fails try the MAC address" option. This removes the dependency on the client's browser and security settings.

SmartConnect Certificate download

In the Certificates step of the Smart Connect Profile Wizard, ensure that you select the complete certificate chain of your uploaded certificate. If all certificates in the chain (from root to server) have been uploaded, then selecting the server certificate will automatically select the entire certificate chain.

- To upload the server certificates, go to **Server > SSL Settings > Server Certificate** tab.
- To upload rest of the chain, go to **Server > SSL Settings > Trusted CA Certificates** tab

CNA Bypass for Android 5.0 +

Devices running Android 5.0 and above introduces system default CP login pop-up windows. To disable this pop-up window enable CNA bypass in the controller.

In the WebUI

Go to **Configuration > Security > Captive Portal** > Advanced Settings section, select Captive Portal Profile and set **Apple Captive Network Assistant** (CNA) Bypass to ON.

Using CLI

Use the **ssl-server cna-bypass** ON command in config mode.

Voice Scale Recommendations

The following voice scale settings are recommended if your deployment requires more than 3 concurrent calls to be handled per AP. The voice scale settings are enabled for an operating channel (per radio). When enabled, all APs or SSIDs operating in that channel enhances voice call service. To enable:

1. In the WebUI, go to **Configuration > Devices > System Settings > Scale Settings** tab.
2. Enter a channel number in the *Voice Scale Channel List* field and click **OK**.

Enable the voice scale settings only if the channel is meant for voice deployment. After enabling voice scale, the voice calls in that channel take priority over data traffic and this result in a noticeable reduction of throughput in data traffic.

IP Prefix Validation

In a situation where a station with an IP address from a different subnet connects to the controller, it can result in various network issues including outage. A new field, IP Prefix Validation is added to the ***ESS Profile*** and ***Port Profile*** configuration page. When enabled, stations with different subnet are prevented from connecting to the controller. By default, IP Prefix Validation in **ESS Profile is ON** and in **Port Profile it is OFF**.

IP Prefix Validation must be disabled if the ESS profile is used for RAC.

New Features

- Virtual Controllers
- Support for Beacon Services
- Spectrum Analysis Support on FAP
- 802.3af support for FAP42x
- 256 clients support for FAP
- Hotspot 2.0 Enhancements
- Change of Authorization (CoA) Enhancements

Virtual Controllers

This release introduces the new FWC-VM Series Virtual Controllers with the following models:

- FWC-VM-50
- FWC-VM-200
- FWC-VM-500
- FWC-VM-1000
- FWC-VM-3000

The Fortinet Virtual Controllers can be deployed on the VMWare, Linux KVM and Windows Hyper-V platforms.

Note:
FWC-VM-1000 and FWC-VM-3000 Virtual Controllers **cannot** be deployed on the Windows Hyper-V platform.

For more information on deploying the Fortinet Virtual Controllers, see the *Virtual Controller Deployment Guide*.

License Management

After completing installation of the Virtual Controller, login to the controller and run the **setup** command to generate the system-id. Perform the following steps to obtain the license.

1. Run the **setup** command on the Controller to generate the system-id, configure the hostname, and configure the static IP address of the Controller, to ensure that the IP address does not change as the system-id/license is mapped to the IP address of the Controller.
2. Save the configuration. The Controller restarts.
3. Run the **show system-id** command to obtain the system-id.
4. Share the Virtual Controller model details, system-id, and the license validity period (or permanent license) with the Forticare Support team.
5. Configure the Virtual Controller instance with the required resources as per the model for which the license has been generated.
6. Install the license from the GUI (See section *Importing and installing a License*) OR from the CLI (Configuration Terminal mode => **vm-license scp://username@<Your file server IP Address>:<license filename>**)
7. Restart the Controller to apply the changes as per the generated license.

Note: A freshly installed system boots up as FWC-VM-50 with default license valid for 30 days.

- System-id is not get generated until you run the **setup** command on a fresh instance.
- System-id is coupled with the IP address. Hence, any change in the IP address generates a new system-id thereby failing validation of the older license. In this case, a new license is required. Changing the IP address via CLI followed by a reboot to activate the new IP address does not generate a new system-id. Hence, license validation fails and the Controller is once again the FWC-VM-50 model. Therefore, use only the **setup** command to change the Controller IP address.
- After the license is invalidated due to a change in the system-id and the controller is once again a FWC-VM-50 model, ensure that you delete the invalid license for the Controller to function properly. Else, the Controller reboots after every one hour.

Importing and Installing a License

Perform these steps to obtain the license using the GUI.

1. Navigate to **Maintenance > System > VM Licensing**
   This image displays a freshly installed system which has a default license (trial based) valid for 30 days from the license issued date.
2. In the **VM Licensing** wizard, click **Import** to add a license. By default, this page lists the license available on the system which includes details on the Virtual Controller model.

License Validation

After the license is imported, validation is performed on the license parameters. If that validation succeeds and the appropriate hardware resources for the requested controller model are allocated, then the license is installed successfully. If either license validation or hardware resource validation fails, the system reverts to the default license. See section *Supported Hardware Configuration* for further details.

Once the license is installed successfully, it replaces the default license. There are two types of licenses – Time Bound and Perpetual (Never ending).

License Monitoring

The license validation happens after every one hour at regular intervals. With 30 days to go for expiry, alarms are raised on the controller. The Software License Expired alarm is generated as per the configured severity. The default severity is critical.

In a fresh installation running on a default license (FWC-VM-50) which is valid for 30 days, you get 30 additional days within which to purchase and apply for a valid license. If a valid license is not imported, at the end of additional 30 days, the Controller will reboot and the APs will go to offline state.

For a system already running on a valid license, the user has 30 additional days following the expiry of the license to renew the license. If the license is not renewed, at the end of additional 30 days, the Controller will reboot and the APs will go to offline state.

To delete a **perpetual** license, select the license and click **Remove License** or run the **delete vm-license** CLI command. After the license is deleted, the Controller reboots and comes up as FWC-VM-50 with the default trial based license.

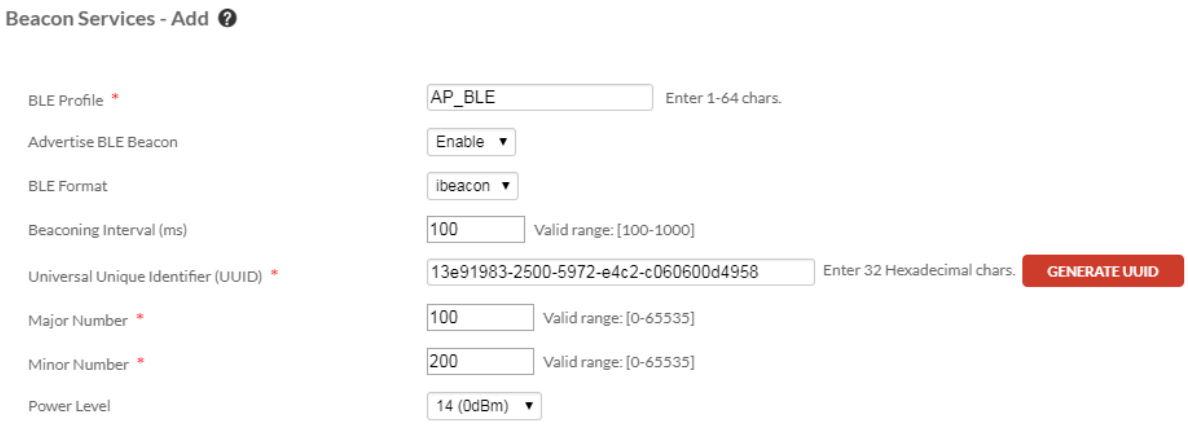
Note: Deletion of trial based license is not allowed.

Support for Beacon Services

Fortinet Beacon Services use iBeacon to allow mobile application (iOS and Android devices) to receive signals from beacons in the physical world to deliver hyper-contextual content to users based on location. Bluetooth Low Energy (BLE) is the wireless personal area network technology used for transmitting data over short distances. Broadly, the Beacon Service requires a Bluetooth based iBeacon device to broadcast signals and a mobile application to receive these signals once it comes in the configured proximity. You can now create multiple Beacon Service profiles and map APs to a specific profile.
The Beacon services are available by default in FAP U421EV, FAP U423EV, FAP U321EV and FAP U323EV. For other non-wave2 APs, you will need Bluetooth adapters (For example: Broadcom USB Class 2 Bluetooth 4.0 Dongle, CSR 4.0 Bluetooth Dongle and Iogear Bluetooth 4.0 USB Micro Adapter GBU521). Ensure that Bluetooth adapters support Bluetooth version 4.0 or above.
Note: Access points must be connected to 802.3at power supply.
You can perform the following operations to manage the Beacon Services. Navigate to **Configuration > Devices > Beacon Services**.

Adding Beacon Services Profiles

This option allows you to add a **Beacon Service**. You can create multiple Beacon Service profiles and also map APs to a specific profile.
APs part of a profile send iBeacons that will help advertise hyperlocal content to users in context to their location.



Update the following fields.

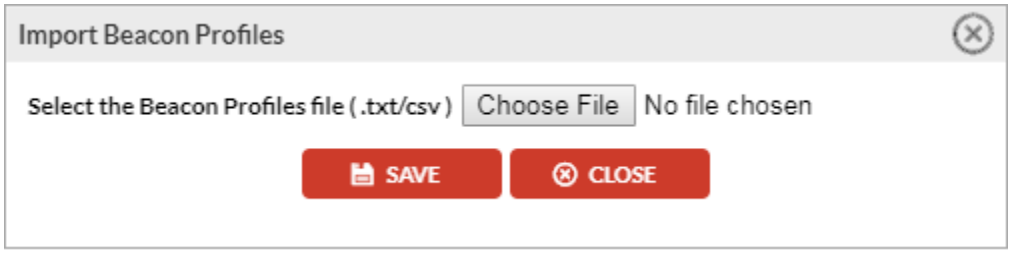
- **BLE Profile** – Unique name for this **Beacon Service** profile. The supported range is 1-64 alphanumeric characters.
- **Advertise BLE Beacon** – Enables the BLE beacons to advertise packets received by devices. These packets determine the location of the device with respect to the Beacon.
- **BLE Format** - BLE Format - Select ibeacon as a BLE Format.
- **Beaconing Interval (ms)** – Select the time interval at which the Beacons transmit signals to associated devices, that is, this sets the rate at which beacons advertise packets. Setting the beacon interval to a higher value decreases the frequency of unicasts and broadcasts sent by the AP. The supported range is 100-1000 milliseconds.
- **Universal Unique Identifier (UUID)** – Click **Generate UUID**, to receive a UUID that is specific to the beacon. The purpose of the ID is to distinguish iBeacons in your network from all other beacons in other networks not monitored by you.
- **Major Number** – This number is assigned to some beacons in a network and is used to distinguish this subset of beacons within a larger group of beacons. For example, beacons within a particular geographic area can have the same major number. The supported range is 0 to 65535.
- **Minor Number** – This number is assigned to identify individual beacons. For example, each beacon in a group of beacons with the same major number, will have a unique minor number. The supported range is 0 to 65535.
- **Power Level** – Select a power level for the beacon's transmit signal. The higher the power the greater will be the range of your signal. This is measured in dBM (Decibel-Milliwatts). The supported range is 0(-29 dBm) to 15(4dBm).

Exporting Beacon Services Profiles

You can export the existing Beacon profiles into your local drive.

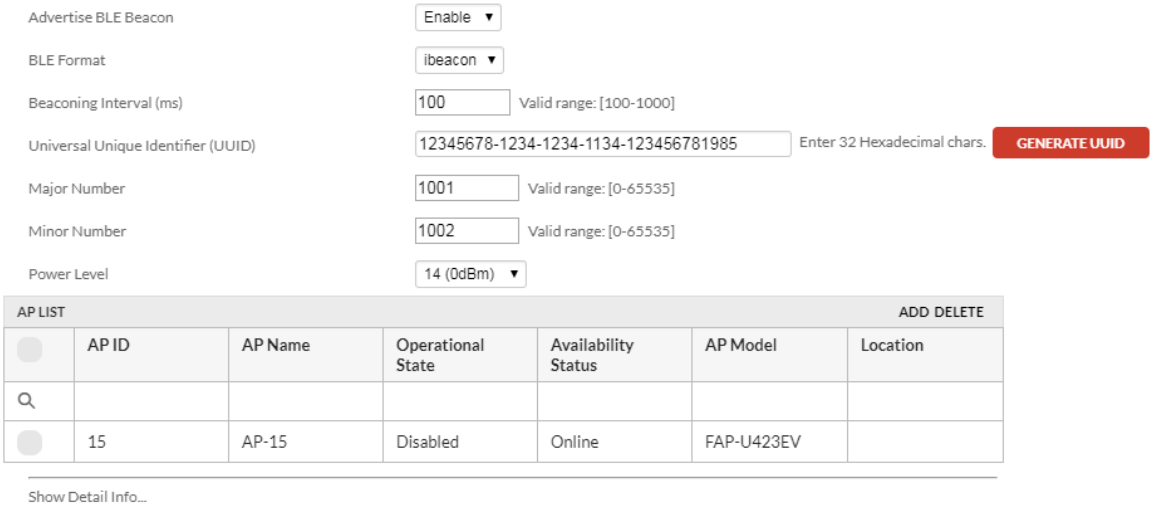
Importing Beacon Services Profiles

You can load Beacon Services profiles by importing files (*.csv) from your local drive. Click **Import** and browse to the saved *.csv template file.



Adding APs to the Beacon Service Profile

Click the edit icon to view the service profile details. **Beacon Services – Update** page is displayed to make changes to the service profile.



Click the **Add** option to start adding APs to the service profile. By default this page shows the list of APs added to the service profile.

- You can add multiple APs to a service profile
- An AP can be mapped to only one service profile at a time

Editing Beacon Services Profiles

Select the Beacon Services profile and click **Edit** to edit the values for an existing profile.

Deleting Beacon Services Profiles

Select the **Beacon Services** profile and click **Delete** in the **Action** column to delete the profile.

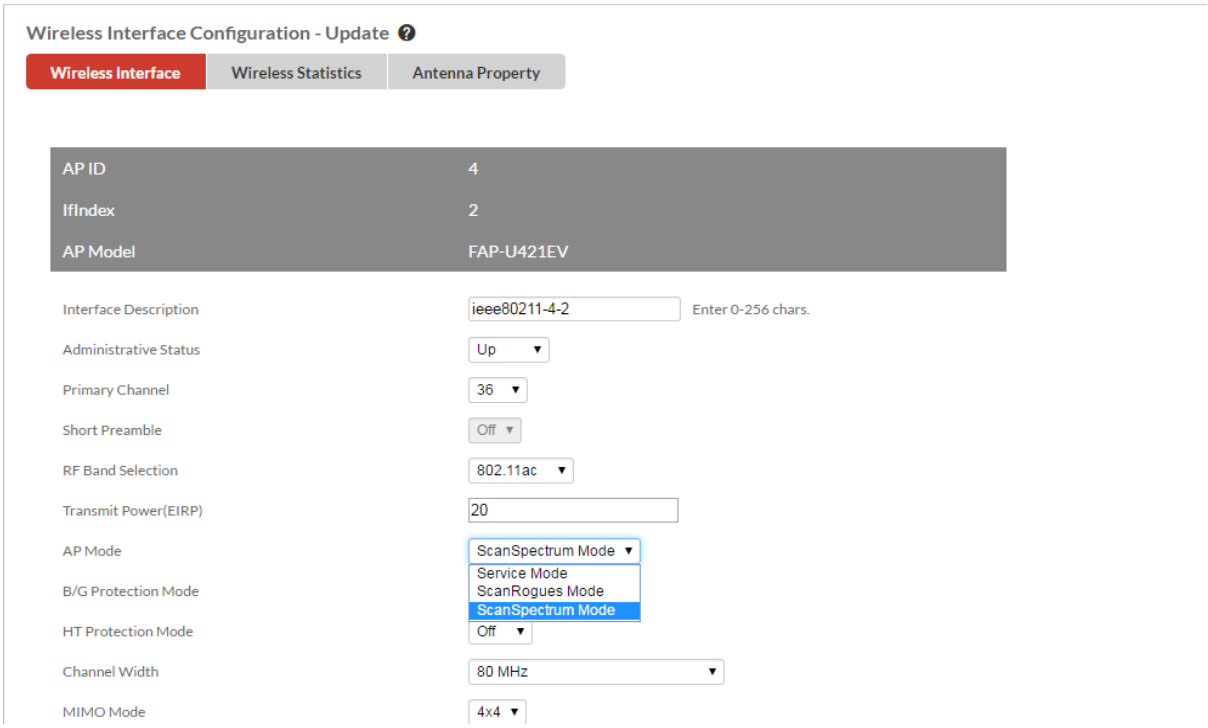
Spectrum Analysis Support on FAP

With this release of FortiWLC-SD, spectrum analysis support for FAP-U421EV, FAP-U423EV, FAP-U321EV, and FAP-U323EV access points with Advanced Interference detection mechanism has been added.

You can deploy these APs in your wireless network scans the environment continuously for interference and sends reports to Spectrum Manager on the interference detected.

Note: The APs need to be discovered in L3 mode for the scan spectrum functionality to work

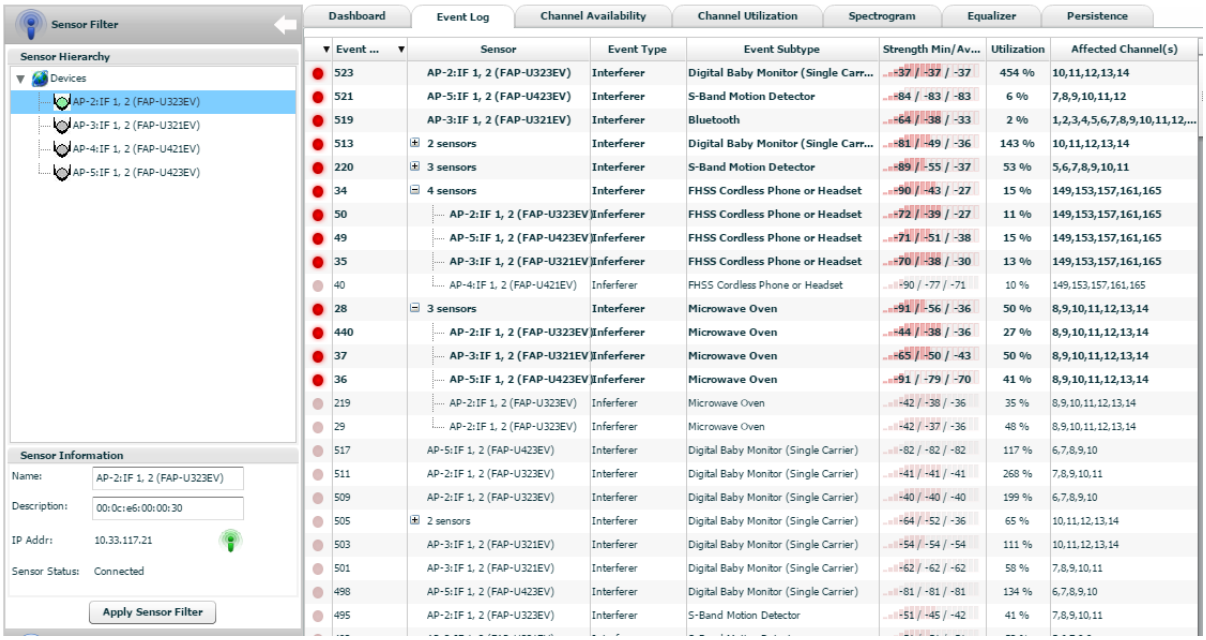
1. Navigate to **Configuration > Wireless > Radios**.
2. Click the edit icon on the radio for the AP which needs to be enabled to scan the spectrum.



3. Change the AP mode from **Service Mode** to **ScanSpectrum Mode.**

Note: The AP will not service clients in **ScanSpectrum Mode**.
Once Scan Spectrum is enabled for a particular radio of an AP, the sensor in that AP starts scanning and reports events to the Spectrum Manager. Each radio interface of the AP scans only the corresponding band (2.4GHz or 5GHz) it is configured for.

Events on spectrum analysis cannot be viewed on the new VM controllers.



Note1: The modification of AP mode from “service mode” to “scan spectrum” mode can be performed by changing the AP Mode from Controller (GUI) or by pushing the AP Template with Radio profile configured “Scan Spectrum” from FortiWLM

Note 2: Users are allowed to configure both radios of FAP-U421EV, FAP-U423EV, FAP-U321EV, FAP-U323EV sensors in ***Scan Spectrum Mode***, which will make the radios to scan both the Radio Spectrum for Interference. For all the other Sensors, Only Single radio can be configured in "*scan spectrum mode*" at a time
Note 3: No Client Service will be provided once radios are in Scan Spectrum Mode

802.3af Support for FAP-U42x and FAP-U32x

With this release of FortiWLC-SD, support for FAP-U42x and FAP-U32x access points powering up when connected to 802.3af PoE source is provided.

- FAP-U42x powered using 802.3af power, will boot up and operate in 2x2 MIMO mode with 17dbm transmit power.
  FAP-U32x powered using 802.3af power works in 3x3 MIMO mode with 20dBm transmit power.
  The USB port will be disabled on these FAPs.
- FAPs powered using 802.3at, will continue to operate in the configured mode with default transmit power.

256 Clients Support for FAP-U42x and FAP-U32x

With this release of FortiWLC-SD, FAP-U421EV, FAP-U423EV, FAP-U321EV, and FAP-U323EV access points can support up to 256 clients per radio interface. The 256 client support per radio is only for a native cell environment. In a virtual cell environment, the maximum clients supported per interface are 170.

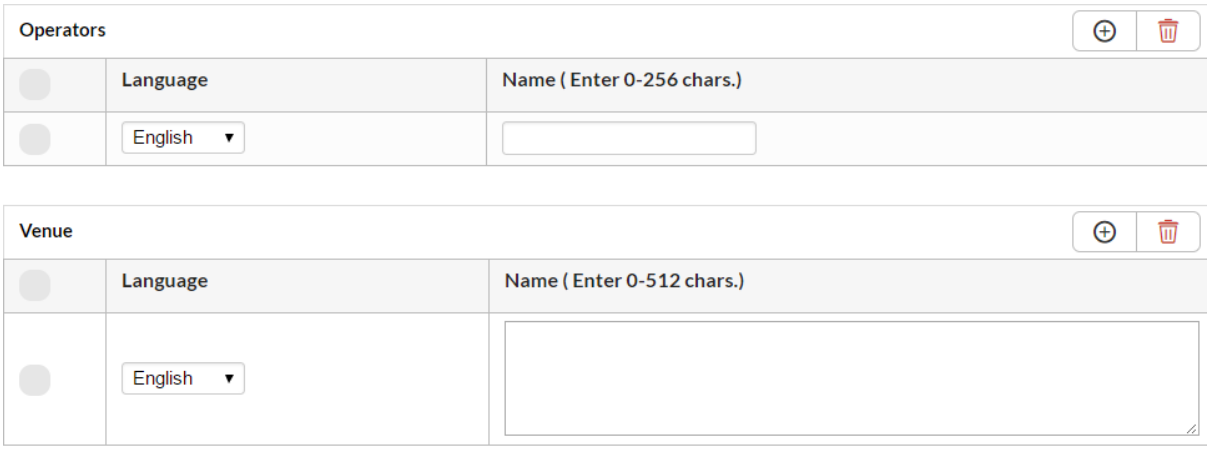
Hotspot 2.0 Enhancements

Hotspot 2.0 is a specification by the Wi-Fi Alliance that specifies a framework for seamless roaming between WiFi networks and Cellular networks. The specification is based on the IEEE802.11u standard; a Generic Advertisement Service (GAS) that provides over-the-air transportation for frames of higher layer advertisements between stations APs and external information servers. This feature will allow users to configure hotspot profiles that can (optionally) be connected to existing ESS Profiles as desired. An ESS-profile connected to a hotspot profile will advertise 802.11u capabilities in its beacons.
FAP-U42x and FAP-U32x are Passpoint R2 certified.

The Hotspot Profiles can be created from the **Configuration > Wireless > Hotspot 2.0** page. By default, the page shows the following details about a Hotspot Profile.

Add Hotspot Profile

1. Select **Configuration > Wireless > Hotspot.**
2. Click **Add.**

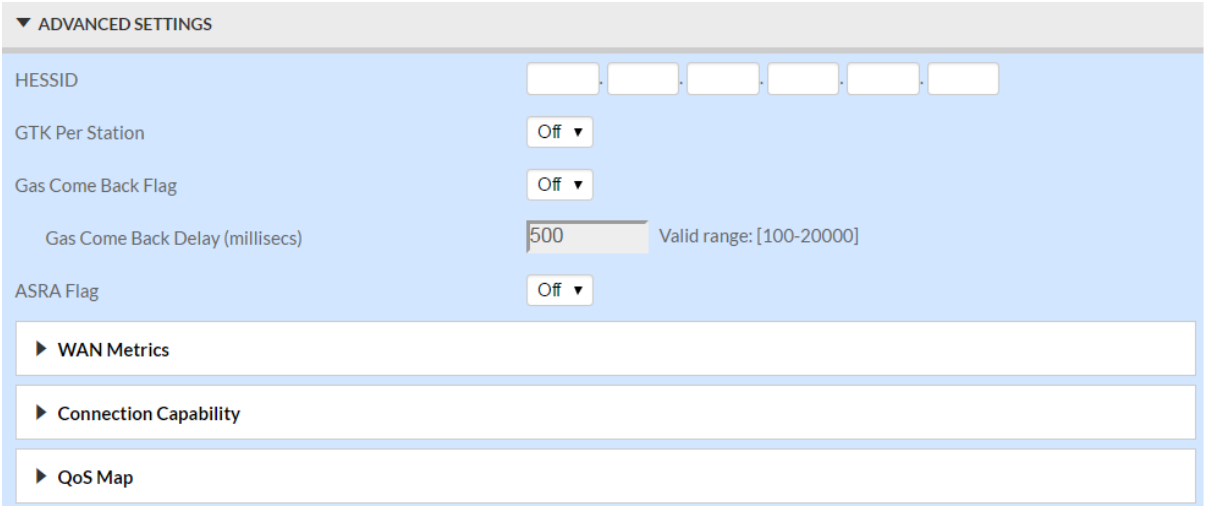


The additional parameters available with this release are:

- Options to add multiple operator names
  - Select Language from the drop down menu
  - Enter Operator Name (0-256 characters)
- Option to add multiple Venues
  - Select Language from the drop down menu
  - Enter Venue Name (0-512 characters)

Advanced Settings

This table describes the advanced Hotspot 2.0 settings.



Field	Description
Advanced Settings	Provide the following configuration details for advanced settings: • **HESSSID -** An AP's Homogenous ESS Identifier (HESSSID), a globally unique identifier, gives a single identifier for a group of APs connected to the same SP or other destination network(s). • **GTK Per Statio**n - Enables the Group

	Temporal Key (GTK) to be assigned per station. • **Gas Come Back Flag** - Enables the Generic Advertisement Service (GAS) comeback request/response option. • **Gas Come back Delay (millisecs)** - At the end of the GAS comeback delay interval, the client can attempt to retrieve the query response using the comeback request action frame. • **ASRA Flag** - Enable the Additional Step Required for Access (ASRA) to indicate that the network requires one more step for access. • **Authentication type** - Configure the network authentication type required as per ASRA. Supported values are, **Acceptance of terms and conditions, On line enrolment supported, http/https redirection**, and **DNS redirectio**n. • **Redirect URL** - Specify the Redirect URL in case of **http/https redirection** and **DNS Redirectio**n.
WAN Metrics	Provide the following configuration details for WAN metrics: • **Link Status State** - Select the status of the WAN link. • **Symmetric Link** – When enabled, the Up Link Speed configured will be applicable to the Download Link Speed. • **At Capacit**y - Select whether the WAN link is at capacity and no additional mobile devices will be allowed to associate with the AP. • **Down Link speed**/**Up Link speed** - The WAN Backhaul link for current downlink/uplink speed in KBPS. • **Down Link load**/**Up Link load** - The current percentage load of the downlink/uplink connection, measured over an interval the duration of which is reported by the **Load Measurement Duration**. • **Load Measurement Duration** - The

	duration over which the downlink/uplink load is measured in KBPS.
Connection Capability	The Connection Capability enables filtering of protocols, allowing or restricting traffic on some protocols and ports. A set of system defined protocols as listed. Additionally, you can also create rules for custom protocols.
QoS Map	Create a Quality of Service (QoS) policy by configuring the following DSCP ranges and DSCP exceptions. • **DSCP Range**s - For a given DSCP range, specify the User Priority (valid range: 0 - 7), DSCP High Priority (valid range: 0 - 255), and DSCP Low Priority (valid range: 0-255). • **DSCP Exceptions** - For a given DSCP exception, specify the User Priority (valid range: 0 -7) and the DSCP Value (valid range: 0 - 255).
OSU Settings	The Online Sign Up (OSU) Service settings configure one or more hotspot providers offering OSU service. • **Online Sign Up Support** - Select to enable OSU. • **OSEN Enable** - Enable OSU Server-only authenticated layer-2 Encryption Network (OSEN) to indicate that the hotspot uses a OSEN network type. This network provisions clients using the OSU functionality. • **OSU/OSEN ESSID** - Specify the OSU ESSID. • **OSU Server URL** - Specify the URL of the OSU server. • **OSU NAI** - Specify the OSU NAI for authentication. Click **Settings** to configure the OSU provider settings. • **OSU Provider Friendly Names** • **OSU Provider Icons** • **OSU Provider Method** - Select one of the

	OSU provider provisioning methods, **OMA-DM** or **SOAP-XML**. • **OSU Provider Description** - The description of the OSU Provider.

Change of Authorization (CoA) Enhancements

With this release of FortiWLC-SD, support for RADIUS based filter-ID and CoA for filter-ID change for MAC authenticated (RADIUS) clients is added.

Enhancements

Patch Management

An AP upgrade.tar patch is created with version string as "SDVersion-XXXXX-Date" where XXXXX is the bug ID. Due to this, there is a version mismatch alarm generated. This was because the version string differed from the controller version (the controller has only "SDVersion" as version string). If the Auto AP upgrade was enabled then the AP would upgrade after every reboot.

With this release, AP upgrade.tar patches will have the version string in the format "SDVersion-BUGXXXXX-Date" to allow the FortiWLC to compare the AP and Controller versions and avoid the above issue.

Fixed Issues

Bug ID	Description
377891	DPI not blocking WhatsApp mobile application traffic for AP822i.
421849	AP sending QOS data before completion of key handshake.
436550	Performance and connectivity issues on AP832 running with Bridge SSID with static VLAN.
422717	MAC filtering with external radius server not working after upgrade to 8.2.
435578	Controller crashing with Oauth.
438963	Sort issue with AP's uptime.
377362	Captive Portal authentication failing randomly.
388777	AP832 losing keepalive and staying in disabled/offline state.
400555	TCP Port 8009 getting dropped when the service control is off and Multicast is on.
421601	Controller not registering the IP address of a Wireless Printer (STA) when a slave is active.
438970/394714/394714	SecurityMM crashes.
440243	AP1020 random reboots.
412860	Passive slave Controller showing no configuration post upgrade.
417159	Hostapd getting stuck and causing connectivity failure for new users.
420165	TIM bit not set on all APs in virtual cell on FAP-U42x.
423600	Reboot getting stuck on 50D until any key is hit.
424187	Configuration loss when wncagent restarts.
424198	Fixed the CLI and UI issues. - System dashboard displays incorrect client count. - The show interfaces Dot11Radio CLI command output does not display the names of the APs along with the IDs. Also, the command output cannot be filtered based on the API ID.
434457	Error during configuring DFS channel 100 on AP822V2.
435046	Printers not being detected through service control. Hence, the service control dashboard shows less printers.
436412	Captive Portal not working with static VLAN bridge mode on AP8xx.
436942	Spikes in the /var/mailbox statistics.
437007	wncagent and hostapd restarts observed in 500D due to redis-server restart.
437013	Captive Portal does not work due to frequent SecurityMM crashes.
437181	Controller is behind the NAT, AP does not come online with CAPWAP.
438540	RADIUS not working with EAP-TLS due to authentication failure.
438749	Not being able to add APs to an ESS-AP table on ESS profile.
438867	High memory usage on 3000D.
439692	AP832 crashing with kernel panic NIP value c02c027c.
439872	Not being able to delete the AP group even when no AP is mapped on to the Controller.
439875	JSON data missing commas in some lines.
439877	Controller being unresponsive while trying to add the APs in ARRP under the

	feature group.
441255	Dashboard displaying incorrect station count.
441278	FortiWLC 3000D hanging at starting the WLAN services.
441519	Station count and throughput dropping to zero on the FortiWLC dashboard.
441521	Controller running out of space.
444103	Most of the devices showing associated with AP ID as '0'on the FortiWLC UI and on the CLI.
445511	EIRP configuration errors.
413366	Client connectivity failure in case of RADIUS MAC authentication failure.
443077	AP not sending association response to SHA256 11w capable clients when 11w, 11r and 11k is enabled in profile.
444379	Network adapters not seen for MC4200-VE, MC3200-VE and, MC1550-VE Controller models during OVA Deployment in ESXi 6.5.
447708	The latest version of Firefox supports automatic captive portal detection for easier access to Wi-Fi hotspots. When accessing the Internet via a captive portal, Firefox will alert users and open the portal login page in a new tab. This feature is available in Firefox 52.0 and above.
443420	SNMP walk with MIB browser fails with timeout error in a scale setup. It is recommended to have an increased timeout threshold and number of retires in a scale setup.
443423	Client certificate authentication failing with Radius EAP-TLS.
436994	When the controller was configured to use **Legacy** feed as the report format, the location server stopped working as there was a change in the RTLS client flag byte.
369350	A difference of 10 dBm in signal strength observed on 2.4 GHZ when the AP operated in the site survey mode.
377253	Changes to honour CoA disconnection requests when a user maps a security profile which is configured for WPA-PSK with MAC filtering enabled, to an ESS profile is implemented.
406337	CoA disconnect requests for Captive Portal (CP) Bypass and MAC filtering enabled stations will have the stations go through the complete MAC and CP authentication while re-connecting.
410131	With Band Steering mode enabled, clients got disconnected after failing MAC filtering and did not get bypassed to the CP page.

Known Issues and Limitations

Bug ID	Description
422724	Two Ethernet ports on a Virtual Controller CANNOT be connected to the same vSwitch. The port group in a vSwitch is configured to be in the promiscuous mode and hence both the ports will receive packets coming from all other ports in that vSwitch, including the other port it is connected to.
415004	VM-FWC-3000D specific: The VMware server decides (randomly) the sequence of enumeration of PCI network device ports. Hence, all the ports should be connected to different vSwitches, whose uplinks should be connected to different ports on the external switch and all those ports should be link aggregated.
435521	For License validation, the eth0 interface should always be up. Due to this limitation Dual Ethernet Redundancy does not work in Virtual Controllers.
424537	Hypervisor limitation - The speed of a 1G port connected to a network interface is always displayed as 10G.
415007	Software License Violation alarm severity will always follow the Controller global configuration of alarms severity irrespective of the remaining validity duration.
437223	The Console page in Chrome indicates that Adobe Flash is not installed even when it is installed in the Spectrum manager. **Workaround:** Enable Flash if the Chrome settings are configured to **Ask first before allowing sites to run Flash** or **Blocked**.
447233	In some cases, if the user tries to connect to the Captive Portal Bypass configured ESSID from any Apple iOS device, a pop-up displays **Unable to join**. After a few successive tries, it gets connected to the ESSID eventually and Captive Portal Login window pops up as expected. This issue exists only with the following configuration: • The device's MAC address is not configured under **MAC Filtering > ACL Deny Access Configuration**. • Under CP Bypass configured ESS Profile, **ACL Environment State** is configured as **Deny List Enabled.** • Station MAC entry is not configured in the RADIUS also.
438782	Spectrum analysis: Overlay interference is misinterpreted as interference detected by the FAP.
446805	When a MAC success client roams from one ESSID to another (both broadcasting same SSID) with CP Bypass and MAC filtering with only local permit-list configured, the user needs to re-login into the Captive Portal.
436573	When upgrading from any prior release to 8.3.3, in N+1 configuration the passive slave controller Switch and Reason are No and No Config respectively. This issue occurs on 64-bit Controller models/instances. **Workaround**: Delete and add the master controller to the passive slave

	controller after upgrading to 8.3.3.
439721	High latency and performance issues in the bridged mode for FAP42x and 32x under static/native VLAN with Vcell configuration. This issue is observed under scale deployments (Corp Wi-Fi), for example, with around 20 APs and 200 clients. **Workaround**: Work around is to configure the ARRP (native cell) for bridged mode deployments.
435490	With Chromecast, applications using SSDP across Vlans are not supported. **Workaround**: • When creating a user group, select **Both** (advertiser and subscriber) as the role and when creating a service control policy, select only **Chromecast** as the service. • When creating a user group, ensure that the advertiser and subscriber have the same AP group and when creating a service control policy, select only **Chromecast** as the service.
447408	The APs do not change channels even when the ARRP and channel plan are enabled.
416989	Degraded IPv4 performance with singe 10GB port when FWC-VM-3000 is deployed on Linux KVM.
443669	The number of stations indicated on the pie charts is incorrect.
449185	CommNodeId is duplicated in multiple Aps in large deployments.
446850	The **conn ap** command connects to the console of a different AP sometimes.

Common Vulnerabilities and Exposures

This release is no longer vulnerable to the following CVE-References:

- CVE-2017-7341
- CVE-2017-7335

Visit https://fortiguard.com/psirt for more information.

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

Contact

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the local contact numbers, or through the Support portal at https://support.fortinet.com/

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service